International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 103-112

AN EFFICIENT MECHANISM FOR SECURE AUTHENTICATION

SHRIKALA M. DESHMUKH[1]& P. R. DEVALE[2]

[1]Research Scholar, College of Engineering, Bharati Vidyapeeth University, Pune, Maharashtra, India

[2]Head of Information Technology Department, College of Engineering, Bharati Vidyapeeth University, Pune, Maharashtra, India

ABSTRACT

After realizing importance of Graphical passwords, In this paper we proposed a system which will overcome all drawbacks of existing systems & will play a great role in password authentication. In this paper we combine the features of D´ej`a Vu, Cued Click Points, Secret Draw technique and Text Passwords. In the password creation process, we provide 4 images. On first 3 images user will select click points and add single digit/text at the place of click point. On the fourth image user will draw a Secret. After password creation, for login to any system, user have to correctly identify the images, correct click points on that images, text/digit entered on that images and the image on which secret is drawn and have to draw the correct secret. If all the images, click points, text/digit and secret is correct, then user will successfully authenticate to the system**.** If any click point, text/digit or secret is incorrect then authentication fails. After the last stage, the message of authentication failed is given.

KEYWORDS: Authentication, Click Points, Graphical Password, Security

INTRODUCTION

Nowadays, one has to authenticate oneself on several IT systems. In early days, text based passwords are used for authentication. The text based passwords are often based upon dictionary words or personal information, resulting in vulnerability to brute force attacks or social engineering. Biometric and tokens are also another methods of authentication but has its own drawbacks such as it requires extra hardware.

Graphical passwords are used as an promising alternative to all these methods, because psychology studied that human brain can recognize images better than the text[6]. Graphical passwords can be classified into three categories:

- Pure recall-based
- Cued recall-based and
- Recognition-based.

Passlogix

It is the Cued recall based graphical password scheme. For password creation user have to click on several locations on an image. For login, users must click on various items in the image in the correct sequence. The Invisible boundaries are defined for each item. It is implemented by passlogix corporation [20].Limited password space & poor passwords are the limitations of this technique.

Pass-Points

Pass-Point comes under click based graphical password scheme. In Pass-Points password consists of sequence of

5 different click points on a single image. The main disadvantage of this scheme are HOTSPOTS [11][12] and pattern formation attacks[13][14].

D´ej`a Vu

It is a recognition-based authentication system, In the D´ej`a Vu system, user have to select certain number of images from a set of images. Later, the user will be required to correctly identify the images in order to be authenticated. The main disadvantage of this system is it is easy for attackers to guess the images.

Cued Click Points

Cued Click Points comes under click-choice based graphical password scheme. Cued Click Points [2] [16] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of authentication failure is displayed after the final click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject(the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point[9].

Persuasive Cued Click Points

Persuasive Cued Click Points comes under click-choice based graphical password scheme. By adding a persuasive feature to CCP [2][16], PCCP [2] encourages users to select less predictable passwords, For password creation PCCP uses terms like viewport & shuffle. To avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses.

Click Draw Based Graphical Password Scheme

There are mainly two steps in this scheme:

- Image Selection
- Secret Drawing.[1]

In first step, a image is selected amongst various images in the image pool. In second step, secret is drawn on the selected image. It has the advantage that In this technique there is not necessity to remember the sequence of clicks. But this system has disadvantage that attackers can guess the image on which secret is done and what type of secret is done.

In our system, for password creation, At first user have to select images from database of images. After that user have to select click points on that images. Then user selects a image on which secret is drawn and draws a secret on selected image. After password creation, for login to any system, user have to correctly identify the images, correct click points on that images and the image on which secret is drawn and the correct secret. If all the images, click points and secret is correct, then user will successfully authenticate to the system**.** Otherwise, if user fails to enter correct password as shown in figure, the message of authentication failed will be given after the final click.

The main advantages of our system are, It will be hard for attackers to guess the correct image amongst various images, correct click points especially secret on particular image. HOTSPOTS and pattern formation attacks are reduced by using features of PCCP (i.e. viewport & shuffle button). By adding feature of secret drawing, attackers fails to know

that there is use of secret drawing technique in between these images, unfortunately if they knows about secret drawing, they don't get exact idea that on which image secret has to be done The message of authentication failed is given after the last stage. It is helpful because it will be hard for attackers to find at which stage their guess is incorrect.

Background

Previously various Graphical Password techniques were introduced. Some of the techniques are given below,

Passlogix

This scheme is designed by Blonder [19].In this scheme password is created by having the user click on several locations on an image. For login, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item. It is implemented by passlogix corporation[20].

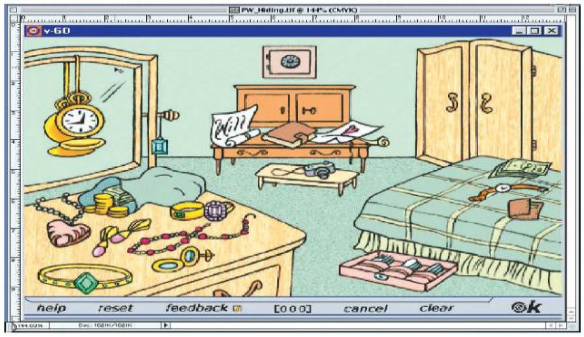


Figure 1: In Passlogix's Graphical-Password System

This technique only provides a limited password space and there is no easy way of preventing people from picking poor passwords.

Pass-Point Scheme

S. Wiedenbeck et al. [5][7][10] proposed pass-point graphical password scheme overcomes passlogix's limitations of needing simple, artificial images, predefined regions, and consequently many clicks in a password. In passpoints on a given image password consists of a sequence of 5 different click points. For password creation user selects any pixel in the image as a click-points and for login the user has to enter the same series of clicks in correct sequence within a system defined tolerance square of original click-points.

The problem with this scheme is the HOTSPOTS [11][12](the area of an image where user more likely to select the click-point) and it is easy for attackers to guess the password because user forms certain patterns[13][14] in order to remember the secret code which results pattern formation attacks are easily possible. Thus the pass-point system suffers from these two major disadvantages. To overcome these disadvantages next technique is to be implemented.

Figure 2: Pass-Points[9]

D´ej`a Vu

Dhamija and Perrig [18] developed, D´ej`a Vu, a recognition-based authentication system, which authenticates a user through his ability to recognize previously seen images. In the D´ej`a Vu system, the user is asked to create an image portfolio by selecting a certain number of images from a set of random pictures generated by a program. Later, the user will be required to correctly identify the images which are part of his portfolio in order to be authenticated.

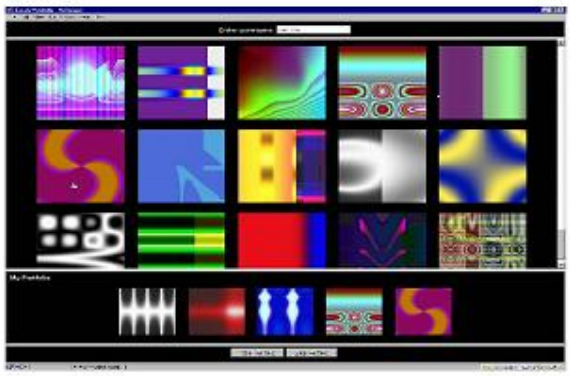


Figure 3: In the Portfolio Creation Phase of D´ej`a Vu, the User Selects Random Art Images from a Larger Set of the Images Stored in the Server [18]

The main disadvantage of this system is it is easy for attackers to guess the images.

Cued Click Points

Cued Click Points [1][2] [16]was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point; it creates a path through an image set. Creating a new password with different click-points results in a different image sequence.

One best feature of Cued Click Point is that the Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks.

But this technique has several disadvantages like false accept (the incorrect click point can be accept by the system)and false reject(the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point[9].

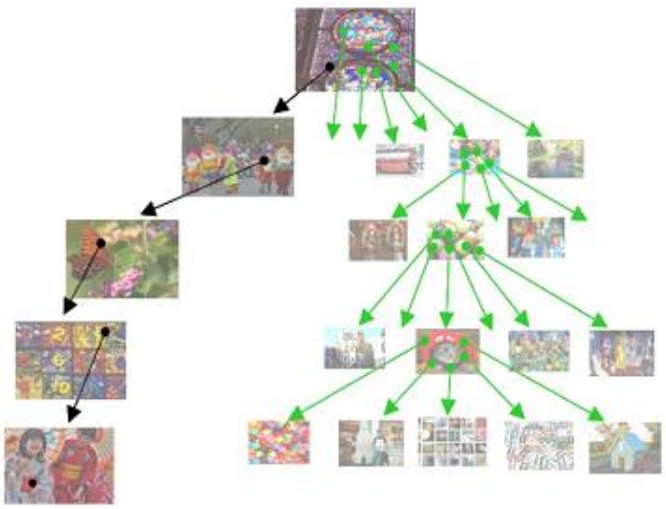


Figure 4: Cued Click Points

Persuasive Cued Click Points

For creating Persuasive Cued Click Points persuasive feature is added to CCP.PCCP [2] encourages users to select less predictable passwords. For password creation PCCP uses terms like viewport & shuffle.

When users creating a password, the images are slightly shaded except for a viewport as shown in the figure to avoid known hotspots the viewport is positioned randomly. The most useful advantage of PCCP is attackers have to improve their guesses. Users have to select a click-point within the highlighted viewport and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport[2]

At the time of password creation users may shuffle as often as desired but it slows the process of password creation. Only at the time of password creation, the viewport & shuffle button appears.

After the password creation process images displayed normally without the viewport & shuffle button. Then user has to select correct click on particular image. PCCP is a good technology but has security problems. Figure shows the password creation process including viewport & shuffle button.

Figure 5: Password Creation in PCCP, Highlighted Area is Viewport (Pool Image is Taken from [15],[2])

Click Draw Based Graphical Password Scheme

The purpose of click-draw based graphical password scheme (*CD-GPS*)[4] is to enhance the image-based authentication in both security and usability. There are mainly two steps in this scheme

Image Selection

In *CD-GPS*, the first step is the *image selection. I*n this step users have to select several images from an image pool. Suppose there are $N1$ images in the image pool, then at first users should select $n \in N1$ images from the image pool in a order and remember this order of images like a story.

Users should further choose $k \in n$ image from the above selected n images. k is nothing but the single image on which we have to draw secret.[4]

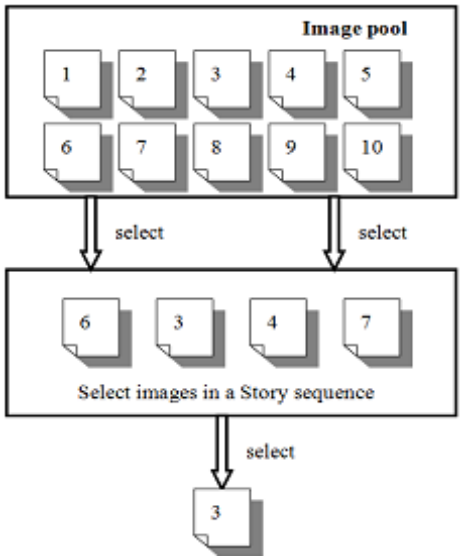


Figure 6: Image Selection in Click Draw Based Graphical Password Scheme[4]

As shown in Figure, there are total 10 images in the image pool i.e.N1 images. Users should first select 4 images from the image pool in a story-sequence i.e. n images(e.g., *{*6, 3, 4, 7*}*).Then users should further select 1 image i.e. k image (e.g., *{*3*}*) from the above 4 selected images to draw the secret.

SECRET DRAWING

This is the second step comes after the image selection. In this step users can freely click-draw their secrets. For constructing secret drawing users use series of clicks

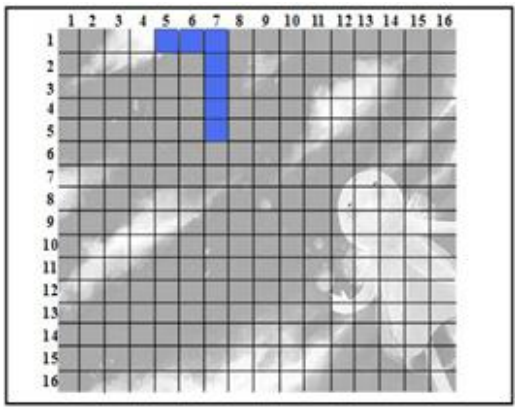
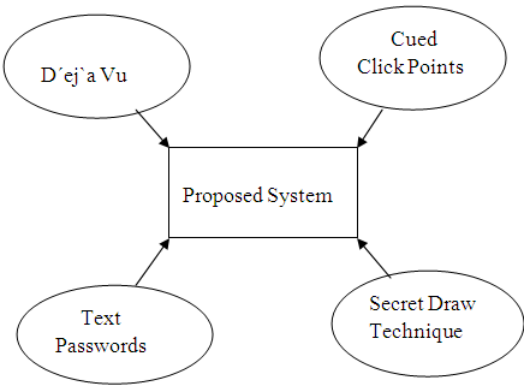


Figure 7: User Draws Number "7" As the Secret

As shown in above figure the image is divided into a 16×16 table. Users can use the coordinate numbers for remembering their drawings. In above figure user draw number "7" as the Secret, which consists of coordinates (1, 5), (1, 6), (1, 7), (2, 7),(3, 7), (4, 7) and (5, 7). In this technique there is not necessity to remember the sequence of clicks. During the authentication, users should re-draw their secrets accurately in the correct coordinates on the image [4].

PROPOSED SYSTEM

In this paper we proposed a system which will overcome all drawbacks of existing systems & will play a great role in password authentication. In our proposed system we are combining features of D´ej`a Vu, Cued Click Points, Secret Drawing and Text passwords.



Existing Systems	Features Used
D´ej`a Vu	Identify sequence of images from database
Cued Click Points	Message of authentication failed is given after the last click.
Secret Drawing	Draw a Secret
Text passwords	Enter text/digit

Figure 8

In our proposed system, if user is new then we provide 4 images to them for password creation. Amongst these 4 images, on first 3 images user will decide its click point and along with click point user have to enter single text or digit at click point but this text/digit should be invisible. On the last image, user have to draw a secret. This is the password creation process.

After password creation, for successful login At first user have to identify these 4 images on which password is created. After that, User have to identify first image, click point on that image and entered text/digit on that image. Then user have to follow same procedure for second and third image. And for fourth image user have to draw correct secret.

If user identifies all images, click points, text/digit and secret correctly then user will authenticate to the system.

SYSTEM ARCHITECTURE

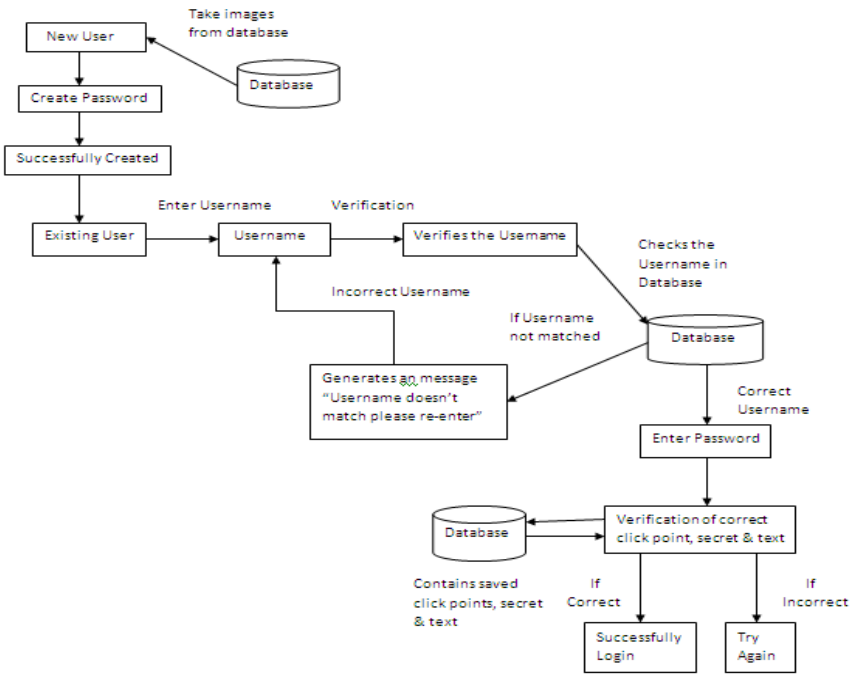


Figure 9

EXPERIMENTAL WORK

Module

Here we have done with first stage of my project. In this first step I developed a database of 20 images. On the user form I have displayed two radio buttons. One is for new user & other is for Existing User. If user is new then our system first asks to enter username. After entering username, User have to click on "Show Images" button. After that system will show 4 images as shown in figure below.

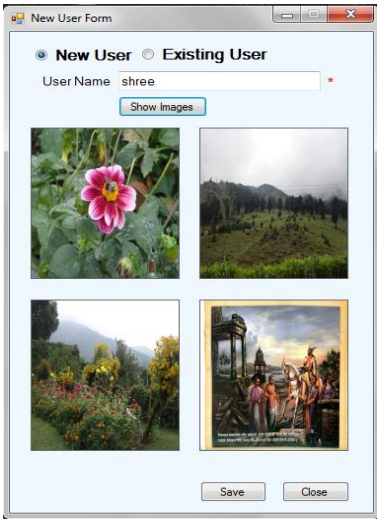


Figure 10

CONCLUSIONS

In our proposed system we combine the features of D´ej`a Vu, Cued Click Points, Secret Drawing and Text passwords. By combining all these features, our system has a great advantage that it is hard for attackers to guess the password means the attackers can't guess on which image they have to enter click point, on which image they have to enter text/digit or on which image they have to draw a secret. Our proposed system will overcome all drawbacks of existing systems.So our proposed system will be the best authentication system.

REFERENCES

1. Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle2"Graphical Password Authentication Using Cued Click Points"1 School of Computer Science, Carleton University, Ottawa, Canada 2 Human-Oriented Technology Lab, Carleton University,Ottawa,Canada(chiasson,paulv)@scs.carleton.ca, robert biddle@carleton.ca
2. Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget,Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE "Persuasive Cued Click Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL 2012
3. Karen Renauda *Department of Computing Science, University Of Glasgowkaren@dcs.gla.ac.uk* "Quantifying the Quality of Web Authentication Mechanisms A Usability Perspective" Journal of Web Engineering, Vol. 0, No. 0 (2003) 000–000_c Rinton Press.
4. Yuxin Meng "Designing Click-Draw Based Graphical Password Scheme for Better Authentication" 2012 IEEE Seventh International Conference on Networking, Architecture, and Storage

5. S.Wiedenbeck, J.Waters, J.C. Birget, A. Brodskiy, and N. Memon. "Pass Points: Design and longitudinal evaluation of a graphical password system". International Journal of Human Computer Studies, 2005.
6. Nelson, D.L., U.S. Reed, and J.R. Walling. Picture Superiority Effect. Journal of Experimental Psychology: Human Learning and Memory 3, 485-497, 1977.
7. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," *Proc. First Symp. Usable Privacy and Security (SOUPS)*, July 2005.
8. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. The design and analysis of graphical passwords. Proceedings of the Eighth USENIX Security Symposium, pages 1–14, 1999.
9. Ms.Uma D.Yadav and Mr. P. S. Mohod, "Enhancement of Knowledge Based Authentication Mechanism using Graphical Password via Persuasion" JOURNAL OF COMPUTER SCIENCE AND ENGINEERING, VOLUME 17, ISSUE 2, FEBRUARY 2013
10. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," *Proc. Third ACM Symp. Usable Privacy and Security (SOUPS)*, July 2007.
11. A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp.Usable Privacy and Security (SOUPS), July 2007.
12. K. Golofit, "Click Passwords under Investigation," Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept.2007.
13. A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc.Ann. Computer Security Applications Conf. (ACSAC), 2008.
14. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.
15. PD Photo, PD Photo Website,http://pdphoto.org, Feb. 2007.
16. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
17. J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
18. R. Dhamija and A. Perrig. D´ej`a Vu: A User Study Using Images for Authentication. Proceedings of 9th USENIX Security Symposium, 2000.
19. G. Blonder. Graphical passwords. United States Patent 5559961, 1996.
20. M. Boroditsky. Passlogix password schemes. http://www.passlogix.com.